Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-30 April 2019

Source: INTERPOL

Date: 22 Apr 2019

INTERPOL deploying team to Sri Lanka to support investigation into bomb attacks

"INTERPOL is deploying a team to Sri Lanka to assist the national authorities investigating the series of bomb attacks at churches and hotels which left nearly 300 dead and some 500 injured. Checks are already being made against the Organization's Stolen and Lost Travel Documents and nominal databases in order to identify potential investigative leads and international connections. Deployed at the request of the Sri Lankan authorities, the Incident Response Team will include specialists with expertise in crime scene examination, explosives, counter-terrorism, disaster victim identification and analysis. If required, additional expertise in digital forensics, biometrics, as well as photo and video analysis will also be added to the team on the ground." READ MORE

Source: The Daily Swig

Date: 26 Apr 2019

Europe remains defiant in its stance against encryption backdoors

"The FBI's latest push to create systems that would provide law enforcement with exceptional access is unlikely to slow down, particularly when its overseas allies – such as Australia and the UK – have passed anti-encryption legislation that paves the way for what feels like Doomsday for privacy advocates everywhere. But over in Europe, the stance on backdoors – or "backdoors by another name" – remains the same: there is no trade-off between security and privacy. That's, at the very least, a belief held by Yves Vandermeer, chair of the European Cybercrime Training and Education Group (ECTEG) – a non-profit organization that develops training materials on subjects such as computer forensics for universities and law enforcement across Europe, the UK, and beyond. "Looking at decryption and encryption, if we respect privacy, then encryption is the main key to security in the IT world," Vandermeer said, somewhat echoing comments made by Wray with the notion that secure communication is a crucial component to our digital infrastructure and, indeed, our rights as citizens. "But we need to address the [encryption] challenge in other ways."" READ MORE

Source: FBI

Date: 22 Apr 2019

FBI, IC3 Annual Report shows Cyber-Enabled Crimes and Costs Rose in 2018

"The statistics gathered by the FBI's Internet Crime Complaint Center (IC3) for 2018 show Internet-enabled theft, fraud, and exploitation remain pervasive and were responsible for a staggering $2.7 billion in financial losses in 2018. In its annual Internet Crime Report, the FBI reports the IC3 received 351,936 complaints in 2018—an average of more than 900 every day. The most frequently reported complaints were for non-payment/non-delivery scams, extortion, and personal data breaches. The most financially costly complaints involved business email compromise, romance or confidence fraud, and investment scams, which can include Ponzi and pyramid schemes. Reports came in from every U.S. state and territory and involved victims of every age." READ MORE

Source: Law Society Gazette

Date: 15 Apr 2019

Away in a hack, reflecting on the Irish cybercrime law

"In May 2017, the then Tánaiste and Minister for Justice Frances Fitzgerald brought forward new legislation in the form of the Criminal Justice (Offences Relating to Information Systems) Act 2017. […] There is little doubt that, following decades of inactivity, it is a welcome step forward that Ireland has finally enacted a single unifying piece of legislation dedicated to dealing with cybercrime. The 2017 act is a long overdue and necessary addition to the law's capacity to tackle new waves of cybercrime. The State is clearly cognisant of the need for legislation and action to address the problems of cybercrime and, together with the publication of the National Cyber Security Strategy and the establishment of the National Cyber Security Centre, Ireland is acknowledging that cybercrime investigation and prevention is a national priority." READ MORE

Source: Daily Sabah

DatFe: 26 Apr 2019

Turkish police detain 15 suspects in nationwide crackdown on cybercrime gang

"Turkish security forces on Friday detained 15 suspects linked to an incident of cyber fraud in which millions of Turkish liras were illegally seized, in anti-cybercrime operations in five provinces of Turkey. The anti-cybercrimes branch of the Istanbul Security Directorate raided properties owned by the suspects in Istanbul, Adana, Zonguldak, Hakkari and Bursa provinces after investigations found that the bank account information of 35 inmates at Metris prison in Istanbul had been illegally obtained." READ MORE

Source: ThreatPost

Date: 29 Apr 2019

2 Million IoT devices vulnerable to complete takeover

"Over 2 million IP security cameras, baby monitors and smart doorbells have serious vulnerabilities that could enable an attacker to hijack the devices and spy on their owners — and there's currently no known patch for the shared flaws. The attack stems from peer-to-peer (P2P) communication technology in all of these Internet of Things (IoT) devices, which allows them to be accessed without any manual configuration. The particular P2P solution that they use, iLnkP2P, is developed by Shenzhen Yunni Technology and contains two vulnerabilities that could allow remote hackers to find and take over vulnerable cameras used in the devices." READ MORE

RELATED ARTICLES

KrebsOnSecurity, P2P Weakness Exposes Millions of IoT Devices, 26 Apr 2019

Source: ENISA

Date: 5 Apr 2019

EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections

"Today the European Parliament, the EU Member States, the European Commission and the EU Agency for cybersecurity (ENISA) organised an exercise to test the EU's response and crisis plans for potential cybersecurity incidents affecting the EU elections. The objective of the exercise, which took place in the European Parliament, was to test how effective EU Member States and the EU's response practices and crisis plans are. It also aimed to identify ways to prevent, detect and mitigate cybersecurity incidents that may affect the upcoming EU elections." READ MORE

Source: The Guardian

Date: 22 Apr 2019

Sri Lanka's social media blackout reflects sense that online dangers outweigh benefits

"The Sri Lankan government's decision to block all social media sites in the wake of Sunday's deadly attacks is emblematic of just how much US-based technology companies' failure to rein in misinformation, extremism and incitement to violence has come to outweigh the claimed benefits of social media. Sri Lanka's government moved to block Facebook, WhatsApp and Instagram – all owned by Facebook – on Sunday out of concern that "false news reports … spreading through social media" could lead to violence. The services will be suspended until investigations into the blasts that killed more than 200 people are concluded, the government said. Non-Facebook social media services including YouTube and Viber have also been suspended, but Facebook and WhatsApp are the dominant platforms in the country." READ MORE

Source: Wired

Date: 17 Apr 2019

Cyberspies Hijacked the Internet Domains of Entire Countries

"Researchers at Cisco's Talos security division on Wednesday revealed that a hacker group it's calling Sea Turtle carried out a broad campaign of espionage via DNS hijacking, hitting 40 different organizations. In the process, they went so far as to compromise multiple country-code top-level domains—the suffixes like .co.uk or .ru that end a foreign web address—putting all the traffic of every domain in multiple countries at risk. The hackers' victims include telecoms, internet service providers, and domain registrars responsible for implementing the domain name system. But the majority of the victims and the ultimate targets, Cisco believes, were a collection of mostly governmental organizations, including ministries of foreign affairs, intelligence agencies, military targets, and energy-related groups, all based in the Middle East and North Africa. By corrupting the internet's directory system, hackers were able to silently use "man in the middle" attacks to intercept all internet data from email to web traffic sent to those victim organizations." READ MORE

Source: Global Risk Insights

Date: 29 Apr 2019

Central Asia: The Land of CyberCrime?

"Currently, only Uzbekistan, Kazakhstan and Kyrgyzstan have made significant inroads into this arena. All three have engaged in the development of comprehensive legal and regulatory frameworks for cybersecurity. Moreover, they have established and adopted "kontseptsiya" or concept papers for the creation of national cybersecurity strategies'. One example of this being the successful Kazakhstan Cyber Shield. They have also formed Computer Emergency Response Teams or CERTs. Additionally, Uzbekistan and Kazakhstan have created dedicated cyber programs at national universities with the intention of training information and cyber experts on domestic CERT agencies. […] Central Asia currently has one of the highest global rates of cyber-criminal activities. This comes despite efforts improving the region's capacity to deal with cyber attacks or cyber terrorism. Kazakhstan, thanks to its attractive financial situation and high number of internet users, has faced significant issues with cybercrime. Statistics indicate that it has had the highest rate of cyber infiltration in Central Asia since 2010. At the same time, 85% of internet users have been compromised. In the past year alone, the Kazakh National Security Committee (KNB) announced that 63,000 attacks have occurred. This shows an increase of 38,000 since 2017." READ MORE

Source: Mondaq

Date: 25 Apr 2019

Data Protection Regulation 2019: An Emerging Frontier In Data Management In Nigeria

"In 2013, the Nigerian Information Technology Development Agency (''NITDA'') issued the Guidelines for Data Protection 2013, but this had a limited impact on the level of awareness and compliance with data protection obligations. This state of affairs along with the increasing economic importance of data, the security implications of misuse of personal data and the EU's publication of the EUDPR necessitated the enactment and release of the Nigerian Data Protection Regulation 2019 (''NDPR 2019'' or ''the Regulation''), which is the first comprehensive and robust effort to regulate the data management sphere in Nigeria. […] The NDPR aims to safeguard the right of natural persons to data privacy, foster safe conduct of transactions involving exchange of personal data and prevent manipulations of personal data. It imposes numerous compliance obligations on data controllers and processors in their collection and processing of personal data of natural persons. The scope of data controllers and processors includes banks and other financial institutions, telecommunication companies, payment gateway companies, internet and IT companies, electoral bodies, data management companies and the Corporate Affairs Commission." READ MORE

RELATED ARTICLES

Naija 247 News, Nigeria plans Internet Code Of Practice to reduce cybercrime, 29 Apr 2019

The Guardian Nigeria, Experts Urge Government to Establish Cyber Security Centre, 17 Apr 2019

Source: Tech in Africa

Date: 21 Apr 2019

Ghanaian Government to Set Up Cyber Security Authority to Fight against Cybercrime

"The Ghanaian Government through the Ministry of Communications announced its intention to fight against cybercrime in Ghana's digital sphere by setting up the Cyber Security Authority (CSA). Ursula Owusu-Ekuful, Ghana's Communications Minister explained that the CSA will report directly to the office of Ghana's President as well as find more sources of funding to aid their work. […] The plan is also followed by the Government's plan to introduce a new Cyber Security Law aims at addressing all cybersecurity-related issues such as child online protection, cyber positive practices, amongst others." READ MORE

Source: Arab News

Date: 27 Apr 2019

Pan-Arab cybersecurity unit to be set up in fight against digital crime

"A pan-Arab cybersecurity unit is to be set up for greater regional cooperation in the fight against digital crime and money laundering, the Saudi Press Agency (SPA) reported. Mohammed bin Ali Kouman, secretary-general of the Arab Interior Ministers Council, said steps were being taken to prevent such crime in the region and to better hold perpetrators to account. These measures included an Arab task force, a cybersecurity unit, and an Arab criminal evidence law that would be adopted by national governments and be a framework for them to amend their legislation on cybercrime evidence." READ MORE

Source: ZD Net

Date: 30 Apr 2019

Vietnam 'on the edge' of becoming a mid-tier cybercrime hub

"Vietnam has the potential to become a mid-level cybercrime hub, according to sociologist Dr Jonathan Lusthaus, who's been studying cybercrime globally for more than seven years. Today's security threats have expanded in scope and seriousness. There can now be millions -- or even billions -- of dollars at risk when information security isn't handled properly. Lusthaus is director of the Human Cybercriminal Project at the University of Oxford, and an adjunct associate professor at University of New South Wales Canberra Cyber. Vietnam has a "very good tradition of hacking" as well as other "technical pursuits", Lufthaus told ZDNet on Monday. "If you look at other parts of South-East Asia, I don't think you always see that same level of interest in technology," he said. Vietnam's economy is growing more than 6% per annum, a figure that's expected to trend upwards of 6.5% through 2020. Money attracts crime and encourages cyber espionage. Cybersecurity firms have already seen a rise of offensive cyber activity from Vietnam through 2018, including the rise of threat groups affiliated with, or even part of, the Vietnamese government." READ MORE

Source: Business Standards

Date: 18 Apr 2019

Journalists in Nepal protest against cyber law

"A group of journalists in Nepal organised a demonstration in Kathmandu on Wednesday, demanding abrogation of cyber law which, they said, is being used to muzzle the voice of media in the country. Nepal Economic Media Society and Online Journalists Association demanded the abrogation of the Electronic Transaction Act. […] The Cyber Crime Act, which came into effect in 2006, has been frequently used against free press, President of Federation of Nepal Journalists Govinda Acharya said. The Cyber Crime Act is meant for authenticating banking transactions and discourage cyber crime, and is not related to journalists or media persons, he said." READ MORE

Source: Apanews

Date: 17 Apr 2019

Liberia allays cyber security threat fears

"Liberia's Ministry of Posts and Telecommunications has assured the business community that the government will ensure that their businesses are protected against cyber security threats in the country. […] He indicated that cyber attacks require a comprehensive and coordinated response and the government has a significant role to play which includes putting the right policy in place, passing the cyber-crime law, data protection and signing on to various cyber conventions including the Malabo, Budapest convention among others." READ MORE

Source: El Comercio

Date: 18 Apr 2019

Peru, Congreso prepara una ley para combatir el cibercrimen

"Luego de que este verano el Perú se haya suscrito al Convenio de Budapest, el primer tratado que establece herramientas de derecho penal y acuerdos de cooperación judicial internacional para combatir el cibercrimen, se ha abierto una agenda legislativa en la materia en el país. Erick Iriarte, del estudio Iriarte & Asociados, detalló que el Convenio de Budapest requiere pasar por un proceso de implementación que implica adecuar la legislación vigente - el Código Penal y la Ley de Delitos Informáticos - a los principios indicados por la Convención." READ MORE

Source: Tele Semana

Date: 24 Apr 2019

Argentina robustece su estrategia de combate contra el ciberdelito

"El ministerio de Seguridad de Argentina alista su Plan de Lucha contra el Ciberdelito, un programa en el que trabaja desde que se aprobó la creación del Comité Nacional de Ciberseguridad. Se trabajará en dos dimensiones: el ciberespacio como transporte de delito y, por otro, como apropiación de bandas criminales para hechos delictivos. Según el portal local iProfesional se seguirán algunos ejes: coordinación federal entre dependencias, cooperación internacional, mejoras en las capacidades forenses, capacitación a fuerzas de seguridad en problemáticas cibernéticas, marco normativo, concientización, prevención y protección de la niñez, entre otros. El Estado contará con la colaboración del sector privado en algunas tareas con el objetivo de encontrar soluciones a la problemática a través de herramientas tecnológicas. En paralelo trabaja en cuestiones como la conformación de estadísticas propias que permitan dimensionar de mejor forma el flagelo y permitir acciones derivadas del buen uso de la información disponible." READ MORE

Latest reports

- G7, Combating the use of the Internet for terrorist and violent extremist purposes, Mar 2019
- ENISA, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 16 Apr 2019
- Malwarebytes Labs, Cybercrime Tactics and Techniques Q1 2019, April 2019

Upcoming events

- 6-9 May, Ankara, Turkey - Case simulation exercises on cybercrime and financial investigations (for North Macedonia and Turkey), iPROCEEDS
- 6-10 May, Banjul, Gambia – Drafting the National Data Protection Policy, GLACY+
- 6-10 May, Praia, Cape Verde – Introductory ToT on cybercrime and electronic evidence for magistrates and prosecutors, GLACY+
- 8-9 May, Bucharest, Romania – Table-top exercise on international cooperation on cybercrime, iPROCEEDS
- 13-14 May, Tirana, Albania – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), iPROCEEDS
- 13-16 May, San José, Costa Rica – Advanced Judicial Training on cybercrime and electronic evidence for judges, magistrates and prosecutors, GLACY+
- 14-15 May, Vienna, Austria – Second Expert Meeting on the joint CoE-FRA Handbook on Cybercrime and Fundamental Rights, GLACY+
- 14-17 May, Ankara, Turkey – Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, iPROCEEDS
- 15-17 May, Bucharest, Romania – FREETOOL showcase workshop in co-operation with University College Dublin, GLACY+ / iPROCEEDS / CyberSouth

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime